"DEVELOPMENT OF VISUAL CRYPTOGRAPIC MULTISECRET SHARING SCHEME FOR GRAY SCALE AND COLOR IMAGES"

स्वामी रामानंद तीर्थ मराठवाडा विद्यापीठ, नांदेड.

Synopsis Submitted To

SWAMI RAMANAND TEERTH MARATHWADA UNIVERSITY, NANDED

For the Award of the Degree of

DOCTOR OF PHILOSOPHY

In Computer Science under the Faculty of

School of Technology

Submitted by

MR. PRAMOD MADHUKARRAO BACHIPHALE

M.Sc. (Computer Science)

Under The Guidance Of

Dr. N.S. ZULPE

M.Sc., Ph.D. (Computer Science)

Principal and Research Guide,

Department of Computer Science

COCSIT, Latur-413512(M.S.)

Research center

College of Computer Science and Information Technology

Ambajogai Road, Latur - 413531 (Maharashtra)

July, 2021

"DEVELOPMENT OF VISUAL CRYPTOGRAPIC MULTISECRET SHARING SCHEME FOR GRAY SCALE AND COLOR IMAGES"

1. Introduction:

Now a day Information Technology sector increases its potential by using powerful tools and technologies which leads progressive growth in communication technologies, further it contributes the major role in interchanging the visual information like images, printed material etc. During process of transferring visual information by using internet, there must be necessity of Security.

Visual Cryptography is technique to encrypt the text, images in such a way that decrypted information appears as image. One of the most important techniques of visual cryptography is secret sharing. Secret image is divided into number of pieces is called as shares and shares are distributed among group. Image is divided into n shares and someone with n share only decrypt image, while n-1 shares not open any information about original image.

Hou Y-C,*et.al.*in 2014 [1] spot light on Cryptography with secret key used to convert data from readable form to an unreadable one. However, there was disadvantage of cryptography which was seen the process of encryption and decryption take more time, hence **Moni Naor and Adi Shamir** [2] spot light on Visual Cryptography because it takes less time and computation.

Visual Cryptography (VC) which also be known as Visual Secret Sharing (VSS), this scheme is used for image security. In this concept of VSS secret image can be encoded into various kinds of *n* shared image afterward it distributed among multiple n participants.

In Visual Cryptography rule the secrete image only can be regained when qualified set of participants overlapped their share unruffled. In general cryptography takes more time and Visual Cryptography is convenient in terms of taking less time and computation.

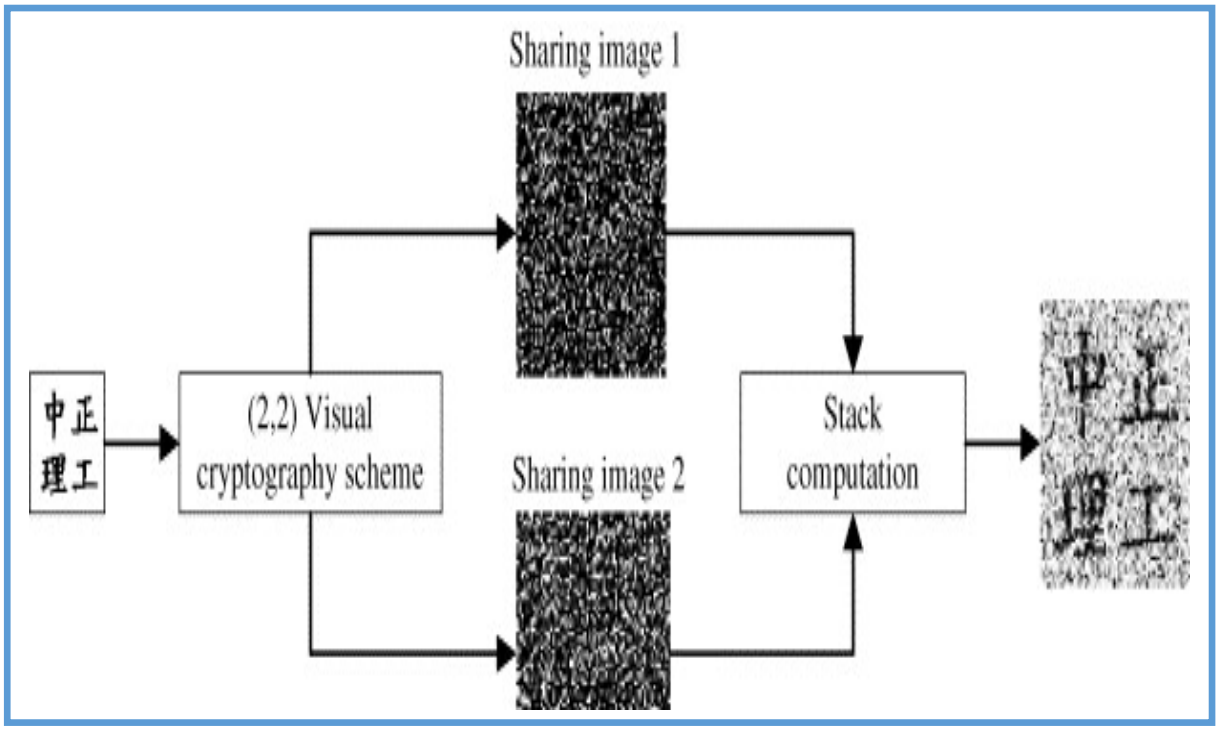


Figure: 1 Basic Visual Cryptography (2, 2) Scheme

Visual Cryptography is technique which can encrypt images without any mathematic operation and decrypt images by human visual capability. There are different scheme of visual cryptography are available in above figure 1 visual cryptography (2,2) scheme is used. This scheme encrypts the secret image in to two images also named as shares and shares are superimposed to get original image. In figure1 Original Image is converted or encoded into two images or shares by using visual cryptography (2, 2) scheme and finally two shares are combined or superimposed to get original secret image Decryption of shares does not require any computation and it require less time.

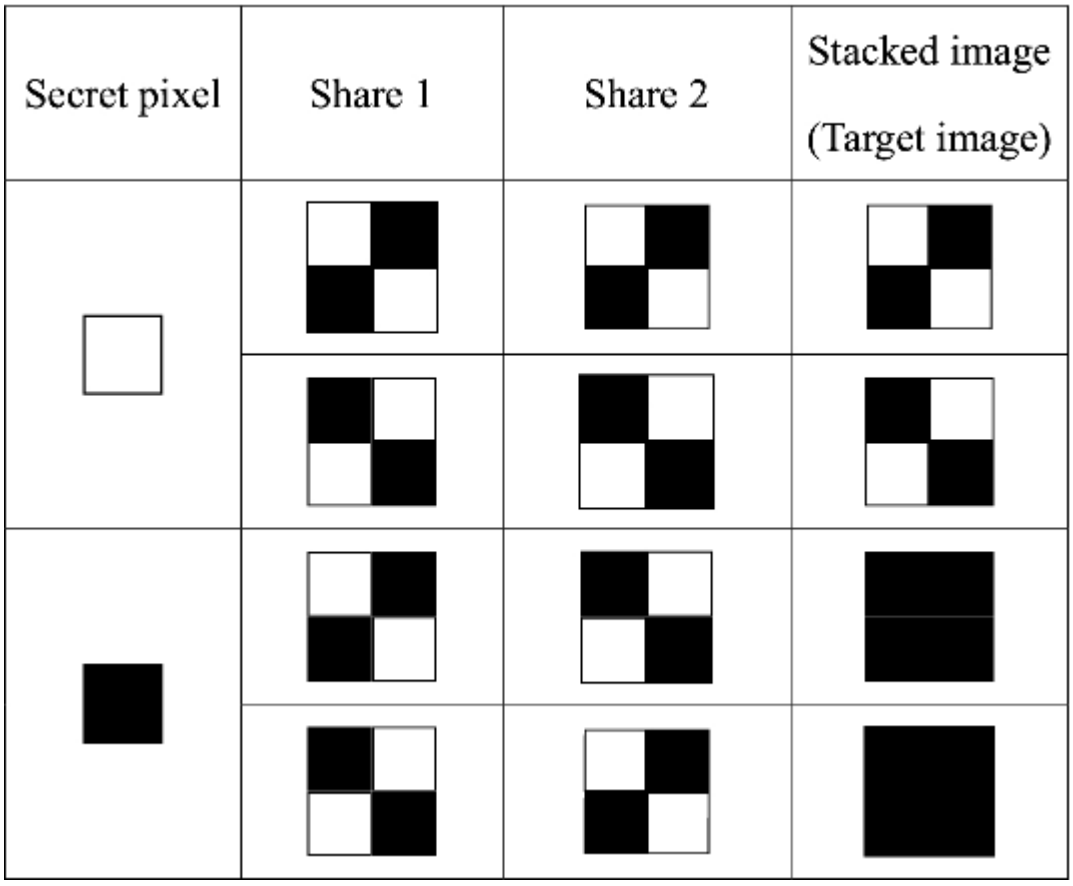


Figure 2: Naor and Shamir (2,2) VC scheme.

Binary image is converted to share1 and share2. In Figure2 shows the one full black pixel and share1 and share2 produced, overlapping share1 and share2 produce original image.

Halftone is technique is used to convert secret image into meaningful and secure image. This method has some drawbacks less quality of image is produced and more memory is required, interference of shared image over retrieved image. Error diffusion is simplest half toning method for improving image quality and reduces computational complexity. This technique is also used for visual colour cryptography where a visual information pixel synchronization and error diffusion method produces shares.

Multiple secret sharing schemes propose that multiple secret images are encoded into two shares and stacked or superimposed in way of shifting. This scheme used with multiple Gray, binary, colour images. Matrix extension algorithm is used with existing visual cryptography scheme having random share can be extended to utilise meaningful share.

2. Review of Literature:

Liu et al. [3] presently had been focused on embedded EVC as beneficial VC schemes which generate meaning-ful shares. He had been noted the results regards embedded EVC scheme based on the distinct design of the dithering matrix by emending the Secret Information Pixels (SIPs) into meaningful cover

Zhou et al. [4] have suggested HVC scheme based on dithering to provide a enhanced visual quality than that provided by EVC. Yet, it is computationally costly due to the circumstance that it inserts the SIPs into pre-existing encoded halftone shares. Also, in using this scheme, a pair of complementary shares is compulsory to prevent the share visual information shown in the decoded image. That is to say, some participants may store more than one share, which may lead to cumulative the suspicion of secret image encoding and the bandwidth.

Wang et al. [5] have suggested HVC technique to improve the image quality of the halftone shares and completely remove the cross interference of the share images on the reconstructed image. This method has capability to concurrently halftone gray scale images and encodes the secret information into the halftone images, instead of modifying halftone images to encode secret information. Usually, in proposed technique, the pixels that carry the secret image information are predetermined formerly the generation of halftone shares. These pixels at next naturally embedded into the halftone shares when the grayscale images are halftoned. In this method, the ED is utilized as the halftoning algorithm to generate halftone shares since it is able to generate a visually pleasing halftoned image with a simple computation. As the location of the secret information pixels is determined by using the image feature of the key complementary pair, the location of the SIPs on other shares are randomly distributed, and this results in producing a poor visual quality

Most of the authors studied on constraint, as **Devi [6]** suggested a worldwide optimization method through all halftone shares based on the void and cluster algorithm, the optimization method mutually rearranges the pixels of the n shares in order to obtain improved overall visual quality of the *n* shares. Without the loss of generality, the shares 1 and 2 are assumed as the key complementary duos among the n halftone shares. Then, the visual quality optimization can be performed on the 3rd, 4th, …. . , n^{th} shares successively.

Further the work extended by **Alex and Anbarasi [7]** applied various techniques of error dispersal such as classical fixed, edge enhancement, green noise and block error diffusion to enhance the image quality of the halftone shares. The quality of the halftone shares is enhanced

by using filters viz. Floyd - Steinberg and Jarvis error diffusion filters. It is noted that the visual quality should be improved.

In order to avoid the distortion and enhance the visual quality of halftone shares, **X. Yan et al. [8]** proposed a HVC scheme with minimum and homogeneously distributed auxiliary black pixels (ABPs). This scheme is designed on the basis of conventional VCS and the binary secret image is encoded into the halftone shares. The access structure of this scheme is a (*k,n),* through embedding prefixed in parallel and maximally separating SIPs into meaningful shares in the half toning process of the cover images by error diffusion. Nevertheless, while it provides a good visual quality, the problem of share's cross interference still unsolved.

Unlike the schemes discussed above, the HVC scheme proposed by **Kumar et al.** [9] is based on EVC using error diffusion filters for half toning purpose. The secret and cover image are both in a gray-level form. In this scheme, the pixel expansion is three times bigger than the secret image, which means more consumption of storage and difficulty in the handling issues.

Mahmoud E. Hodeish et.al. [10] have studied an optimized halftone visual cryptography scheme using error diffusion, they used error diffusion for halftone processing and elimination of HVC constraints such as explicit requirement of code book, random pattern of shares , by considering smallest possible halftone cell size. The construction scheme security was assured by following VC basic principal and for better visual quality production XOR operation is employed in decoding process. It was observed that the resultant recovered images were free from cross interference. The effectiveness of proposed work was supported by statistical analysis through objective evaluation matrices and also this work can decrease the complexity to enhance possibility for different high quality practical application. Importance of this proposed work is In development of (*k,n*) general access structure for HVC.

Daoshun Wang et. al.[11] have explored Probabilistic visual secret sharing schemes for grey-scale images and color images. Visual secret sharing scheme is technique used to encrypt image and decrypt by using human visual system for recovering the original image. Pixel expansion creates large and less quality image. A number of probabilistic VSS scheme for binary image have been proposed with less pixel expansion. This proposed scheme general probabilistic (k,n)-VSS scheme for grey-scale images, another scheme for color images. Pixel expansion initialize by user defined value, user defined value is 1 then there is no pixel expansion and quality of secret image calculated by average contrast, is equal to existing deterministic VSS schemes.

Feng Liu et. al. [12] has stated that Step construction of visual cryptography schemes. Two main drawback of visual cryptography scheme are large pixel expansion for share image and less contrast for constructed image. Proposed scheme construct VCSOR and VCSXOR for general access structure applying (*2, 2*)-VCS repeatedly where participant can get multiple secrets images. These techniques reduce the average pixel expansion.

Arun Ross et. al. [13] has proposed Visual Cryptography for Biometric Privacy. This work stated use of visual cryptography for biometric data such as face images, private face image is dithered into two host images, these two images are stored in two separate database servers such that original image is constructed if both host images simultaneously available.

Mahmoud E. Hodeish et.al. [14] Have explored a new XOR based visual cryptography scheme for authentic remote voting system. The recent technology demands high security, verifiability in case of remote voting system for stop cheating process in election using internet. A new scheme is developed to authenticate user of RVS by using new matrices, X-OR operator. This system uses mean square error, peak signal to noise ratio for verification process. Proposed scheme has less computational price and provides balance between security, storage and performance.

Prasad Pawar et. al.[15] has stated that Visual Cryptography in Internet Voting System where researcher use Visual Cryptography for generating password by combining two shares.

First share is sent by administrator on email of user and second is available at the time of election. If hacker gets one share out of two it will not possible to generate password. This system provides security to online system by sending mail to user.

Tuyls, P. et.al. [16] have explored XOR-based Visual Cryptography Schemes based on polarisation of light. This work is based on X-OR operation and it has good contrast, colour, and resolution. He developed X-OR based scheme with Threshold Visual Cryptography. They show that n out of n schemes with ideal resolution and contrast exist, and that (2, n) schemes are corresponding to binary codes. This scheme is best contrast and resolution than or based scheme.

Y.-F.Chang. [17] has stated new data hiding scheme using pixel swapping halftone images and decryption requires no computation. This proposed scheme generates secret image by overlapping the stego-image with another halftone image and provide high quality image without losing characteristics of original image. These techniques provide data hiding and cooperate with other data hiding scheme.

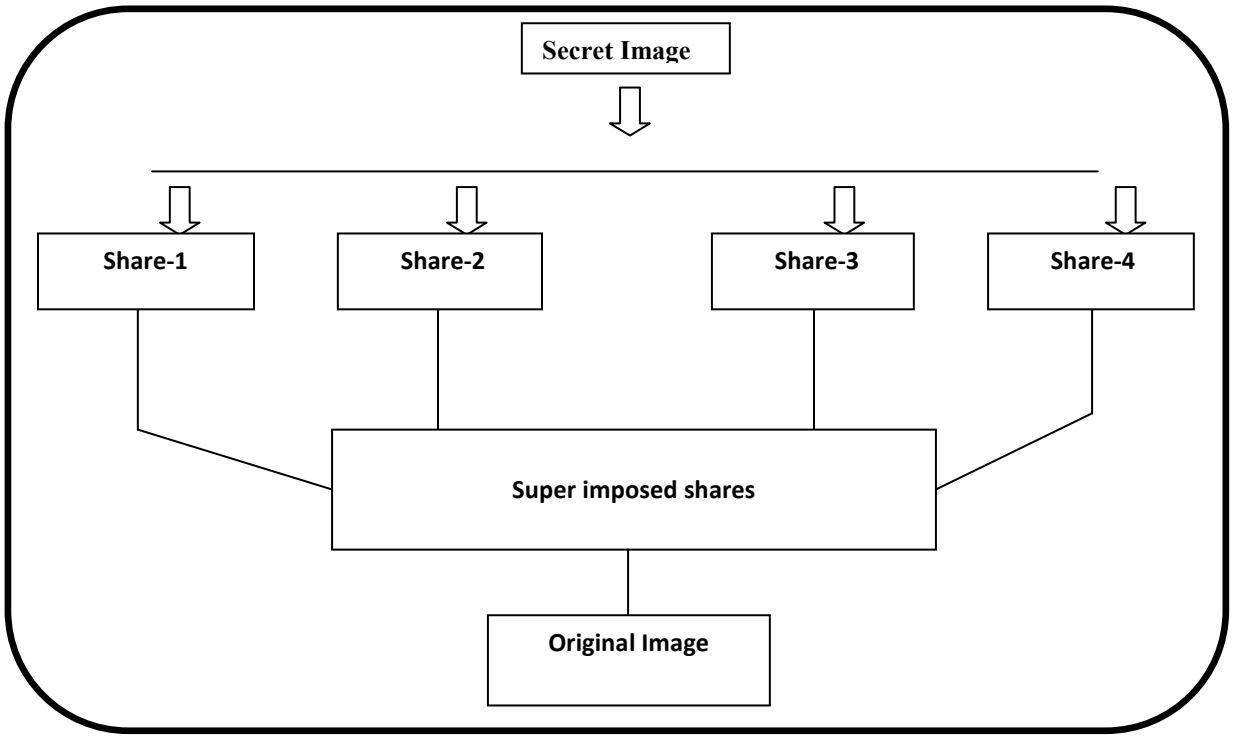
D. R. Somwanshi. et.al. [18] have explored a contrast optimal visual cryptography for halftone images. The proposed scheme can share secret halftone image to n number of users and user can reveal the secret by overlapping n secret images. The user having n-1 secret halftone image could not reveal the secret. This method proposes noise like share, the share size and recovered original image size is same and reduces pixel expansion design on code book and matrix transposition. This scheme shares black and white gray image and generate correct result and also reduces complexity, solves security issues.

3. Objectives of Research:

1. To reduce the pixel expansion occurs while superimposition of shares
2. To reduce the execution and transmission time
3. To work on gray level images and generates meaningful share
4. To work on multi secrete image sharing

4. Methodology to be adopted:

1. Input- secret grey level image.
2. Apply the Jarvis's Halftone algorithm for converting image into halftone image
3. Initialize n shares as per the requirement
4. Define code matrix for creation of shares and create shares
5. Implement multi secret visual cryptography scheme and Halftone visual cryptography scheme
6. Super imposition of shares to generate the original image
7. Statistical analysis of result and comparison with existing system.



5. Importance of study/ Society application:

i. International status.

Today's world is world of internet where all the companies and organizations are sharing information in the text and image format.

Online System most of the textual and image information is transferred. There is need of information security that can be achieved by visual cryptography. Information secured and transferred and recovered by visual cryptographic schemes.

ii.National Status.

Many governments as well as private organization such as schools, colleges, offices etc. uses biometric, electronic mail, servers and computers for storing and identifying their information and share the information.

Data of organization is secured by different visual security techniques.

iii. Significance of the study.

Visual Cryptography Research is done mainly for Information security and hiding information. Most of the information (image, text and files) shared securely on network only authenticated user can access original information.

1. **Biometric Security**

   Biometric is effective identification and authentication technique for employees of company and institute. Biometric data secured by visual cryptography image sharing technique

2. **Steganography**

   Steganography is technology to hide secret data by implanting it into an image. It is most effective method used with cryptography for additional security of data. Steganography used in health care, military for secret communication between two parties.

3. **Water Marking**

   Watermarking is technique where text, logo is added into image which explains about copyright and ownership of information or document. This technique protects data from unauthorized use and intellectual property right.

4. **Human machine identification**

   Visual cryptography plays an important role in differentiate the machine and human. Online system needs to identify human and machine by sending images like captcha, QR-code etc.

5. **Electronic voting system**

   Electronic voting system is technique where data must be stored on server, there is chance of data stolen or hack for protecting data there must encryption and decryption techniques used.

6. Proposed Work Design/Formulation and structure of study:

Tentative month wise plan of planned study is designed as per the suitability of the study.

First Six-Month Plan

1. Study and Review of different visual cryptographic schemes
2. Study of binary visual cryptographic scheme
3. Study of Gray level visual cryptographic scheme
4. Study of halftone visual cryptographic scheme

Second Six-Month Plan

1. Design of codebook for creation of shares.
2. Study and implementation of (2,2) binary visual cryptography scheme

Third Six Month Plan

1. Study and implementation of halftone visual cryptography scheme

2. Design of new optimized visual cryptography scheme for Gray level images
3. Paper publication of proposed method

Last Six-Month Plan

1. Result discussion and statistical analysis of proposed method.
2. Thesis Writing.

7. References:

1. Hou Y-C, Wei S-C, Lin C-Y (2014) Random-Grid-Based Visual Cryptography Schemes. Circuits and Systems for Video Technology, IEEE Transactions 24(5):733–744. https://doi.org/10.1109/TCSVT.2013.2280097
2. Moni Naor & Adi Shamir A (1994) Visual cryptography. In: Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, pp 1–12.
3. Liu F, Wu C (2011) Embedded Extended Visual Cryptography Schemes. IEEE Transactions on Information Forensics and Security 6(2):307–322. .
4. Zhi Z, Arce GR, Di Crescenzo G (2006) Halftone visual cryptography. IEEE Trans Image Process 15(8): 2441–2453. https://doi.org/10.1109/TIP.2006.875249
5. Wang Z, Arce GR, Di Crescenzo G (2009) Halftone Visual Cryptography Via Error Diffusion. IEEE Transactions on Information Forensics and Security 4(3):383–396. https://doi.org/10.1109/TIFS.2009.2024721009
6. Sangeetha Devi E (2010) Enhanced visual secret sharing scheme via halftoning technique. 2010 International Conference on Communication Control And Computing Technologies, Ramanathapuram: 769–776. https://doi.org/10.1109/ICCCCT.2010. 5670 739
7. Alex NS, Anbarasi LJ (2011) Enhanced image secret sharing via error diffusion in halftone visual cryptography. 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari: 393–397.
8. Yan X, Wang S, Niu X, Yang CN (2015) Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. Digital Signal Processing 38:53–65
9. Kumar P, Agarwal S, Shivani S (2014) Halftone Visual Cryptography with Pixel Expansion through Error Diffusion. International Journal of Information & Computation Technology 4:1419–1427
10. Mahmoud E. Hodeish, Vikas T. Humbe(2018) Multimed Tools Appl, 77 24937–24953.
11. Daoshun Wang, Feng Yi, Xiaobo Li (2011) Probabilistic visual secret sharing schemes for grey-scale images and color images, Information Sciences 181:2189-2208.
12. Feng Liu, Chuankun Wu, Xijun Lin(2010), "Step Construction of Visual Cryptography Schemes," IEEE Transaction on Information Forensics and Security 5:27-38

13. Arun Ross ,Asem Othman (2011) Visual Cryptography for Biometric Privacy,IEEE Transaction on Information Forensics and security 6:70-81.
14. Mahmoud E. Hodeish, Vikas T. Humbe(2017)A New Xor-Based Visual Cryptography Scheme For Authentic Remote Voting System ,International Journal of Engineering Sciences & Emerging Technologies 9:95-101
15. Pawar, P., Pansare, T., Shinde, J., Shinde, S., & Suryavanshi, P (2015) Visual Cryptography in Internet Voting System, In International Journal of Computer Science (IIJCS) 3: 1-4.
16. Tuyls, P., Hollmann, H. D., Lint, J. V., & Tolhuizen, L. M. G. M. (2005) XOR-based visual cryptography schemes. Designs, Codes and Cryptography 37: 169-186.
17. Y.-F.Chang,J.-B.Feng,,C.-S.Tsai,Y.-P.Chu,H.C.Syu (2008) New data hiding scheme using pixel swapping halftone images, The Imaging Science Journal 56:279 -290.
18. D. T. Somwanshi and Vikas T Humbe,(2020) "A Contrast Optimal Visual Cryptography Scheme for Half-tone Images", International Conference on Recent Trends in Image. Processing and Pattern Recognition, Communication in Computer and Information Science (CCIS), Springer Nature.

Research Scholar	**Research Guide**
Mr. Pramod M. Bachiphale	**Dr. N.S. ZULPE**